INFORMATION SECURITY FY2006

If you have questions regarding Information Security, you may telephone Dr. Herb Doller, Information Security Officer at 214-857-0512

1) You should report all information security incidents. You should know what constitutes a security incident. VA North Texas Health Care System (VANTHCS) staff, contractors and volunteers are to report known or suspected incidents by telephone to the VANTHCS Information Security Officer (Herb Doller, Ph.D., extension 70512) or to the Information Resource Management Service Help Desk, (extension 74357 or 7HELP).

An information security incident is something that can have a damaging effect on a computer or other information system. Examples of security incidents include computer virus infections, compromised passwords, attempted or actual break-ins of information security systems and theft of information.

You should not discuss actual or suspected incidents involving information security with the press or anyone other than approved VANTHCS staff.

2) It has been said that your password is like a toothbrush, you should change it at least every 90 days and it should never be shared.

It has also been said that your password is like bubble gum. It is strongest when fresh and should only be used by one person. If you leave it laying around, there's an excellent chance that you'll have a sticky mess.

The Department of Veterans Affairs (VA) requires passwords to be at least eight (8) characters long, contain at least one letter and a number or special character and be changed every 90 days.

One suggestion for selecting a "strong" password is to think of a phrase that contains at least seven words and a number. Use the first letter from each word and the number as your password. For example, "My children study math 7 days a week". The password would be Mcsm7daw.

3.) Attacks on computers can be made by deceiving you or an administrator by pretending to be a "network official". They may ask you to verify your user and access code thereby gaining information to access the computer system. This is a social engineering technique.

Social engineering techniques can also involve the use of Java Applets. A Java apple is a computer program that can be sent along with a web page to a user. For example, an attacker/hacker could insert a pop-up dialog box stating that you have been "logged off" and that you must re-enter your identification (ID) and password. However, the network connection hasn't really been lost and now your ID and password have been Compromised.

Many attackers use social engineering techniques because people are usually unsuspecting and want to be helpful. Hackers/attackers have been known to go through an organization's trash/dumpsters, pose as a technician or call a "computer assistance help desk" to obtain information so that they may gain access to your computer system. The important thing to remember is not to give sensitive information to anyone.

4.1) The most important thing to remember about data is to have backup data. Three important points to make about backup data are as follows:

You are responsible for making backup files of your data. The data stored in your VHANTXHOME/ID directory has backup files made every night by Information Resource Management Service.

- Your backup data files should be kept current and you should be sure that you are able to open them.
- Backup files should be properly stored and secured to prevent unauthorized access to the information on the files. You might consider storing your files in a locked file cabinet or in a locked room. In the event of fire or some other catastrophe, it may be advisable to store information in another secure location.

5.) There are three R's of e-mail: RIGHTS, RISKS and RESPONSIBILITIES
The VA has the RIGHT to monitor all information systems to include e-mail. Sending an e-mail message has RISKS because your message can be compromised. E-mail is not a private method of communication nor is it secure. You must take RESPONSIBILITY for your e-mail transmissions. Respect copyright laws and never send illegal transmissions.

6.) A computer virus is a program that makes copies of itself and transfers to other computer systems. A virus can damage files on your computer or render your computer useless. E-mail messages with attachments represent particular problems. Messages with attachments from someone unknown to you should be deleted to prevent a virus attack to your computer.

Anti-virus software should be installed on your VA computer to protect your computer from viruses. If a known virus is circulating, IRMS will alert VANTHCS employees, who are then expected to delete the message without opening or reading the message. The message must be deleted both from the In Box and the Wastebasket.

7.) It is the policy of the VA to use only software licensed by the VA. The use of unauthorized software may lead to disciplinary action.

Most license agreements allow you to make only one backup copy of software. Some licenses allow for single-user, non-simultaneous use. For example, you can have the software on your computer and laptop as long as both are not in use at the same time.

8.) All employees, contractors and volunteers have a responsibility to be familiar with VA security policies, procedures, rules and regulations.
These include the following:

- Do not install software on your computer that is not authorized as essential to the accomplishment of your official duties.
- Avoid the urge to e-mail sensitive information just for the sake of convenience.
- When your workstation begins an update of its antivirus software, let the update process finish before initiating other work on your computer.
- Only use authorized virus scanning software on your computer. Know the source of any computer software such as diskettes or files before you download them into your computer. Be sure to scan all files for viruses before you use them.
- Learn as much as you can about information security. The people who use computers are the most important computer security "system" at the VA North Texas Health Care System. Their support can greatly enhance the effectiveness of the Information Security Officer (ISO).

9.) Employees who use computers incur additional responsibilities to include:

- Reporting known or suspected improprieties involving computers to your
- Information Security Officer (ISO).
- Using government computers for lawful and authorized purposes only.
- Properly selecting and securing your passwords. Passwords are to be changed every 90 days and should not be shared with anyone.
- Ensuring that your computer files have backup files and that they are properly stored and secured.
- Complying with all government policies and procedures for using computers and computer software.
- Using only authorized virus scanning software on your government computer. All computer software files should be scanned before use.
- Complying with the terms of any software license that may involve your work with the government.
- Learning as much as you can about information security to safeguard government computers and information systems. With your help the effectiveness of the ISO is significantly enhanced.

10.) You should never generate or send offensive or inappropriate e-mail messages, graphical images or sound bites. E-mail messages should be limited to only those individuals that need to receive them. All computer files should be properly classified and protected. You may do this by labeling sensitive information, logging off your computer when leaving your work site and by encrypting sensitive information that you forward over the Internet.